Bono Mack revises data breach bill

JOHN SHINKLE/POLITICO

Rep. Mary Bono Mack's new proposal includes tweaks meant to alleviate concern from Democrats.

By TONY ROMM | 7/19/11 10:48 AM EDT

The House commerce subcommittee led by Rep. Mary Bono Mack (R-Calif.) has scheduled a markup for Wednesday on a revised version of her bill to require companies to boost their data security practices and notify consumers in the event of a breach.

The chairwoman's new proposal, circulated among stakeholders leading up to Tuesday's announcement, includes a number of technical and substantive tweaks meant to address problems raised at a June hearing on the bill and to alleviate concerns among some subcommittee Democrats.

However, it is unclear whether the changes have earned Bono Mack any Democratic co-sponsorship. A spokesman for the subcommittee was not available for comment early Tuesday.

Entering the markup, the most significant tweaks to the bill involve how companies that have had their computer systems hacked would be required to notify consumers in the event of a data breach. In a previous version of the bill, a hacked firm would have been required to notify consumers and the FTC within 48 hours after assessing the "scope" of an incident — a phrase some Democrats felt was too open ended, and allowed companies potentially to delay notification indefinitely.

The new version remedies that concern by requiring companies to notify consumers "within 48 hours after identifying individuals whose personal information was acquired or accessed," according to a GOPmemo provided ahead of the hearing.
A company may not have to notify consumers at all, however, if it makes a "reasonable determination" that any breach does not present "reasonable risk of identity theft, fraud or other unlawful conduct," according to the memo.

The revised draft would cap the time a company could assess the impact of a breach and notify consumers.

Companies would also have to inform law enforcement "without unreasonable delay" of any hacking incident. That's also a change from the earlier version, which gave affected entities 48 hours to comply.

Still another change to the bill clarifies that a breach on a third party holding data for another firm would require that third party to only "notify its direct customer." It's those individual businesses that must then inform their consumers about a server intrusion. That would seem to make clear that a hacked company such as Epsilon would notify its business partners, such as Target or Best Buy, and those companies would then alert affected users.

Further tweaks to Bono Mack's proposal are found in the information security portion of the bill. One revision puts into legislative language the idea of a "sliding scale" for companies based on how many users they serve and the type of data they hold.

Yet a number of the bill's key provisions remained substantively untouched. The bill would still task companies to develop plans for data minimization — the idea that companies must limit the personal information of customers they retain for specific business purposes. The FTC would not be able to set any standard for data minimization, but the agency could still take aim at a company if it did not adhere to its own plan. And the bill would still apply to nonprofit organizations, as well as to other organizations designated as 501(c) by the IRS.

The bill still does not apply to entities already covered by sector-specific security and data laws, such as the Gramm-Leach-Bliley Act or HIPAA. That said, the new version of the bill clarifies that those under GLBA and still subject to FTC jurisdiction would have to comply with some parts of Bono Mack's new data security proposal.